

System Wide Information Management (SWIM)

Interoperability Basic Security Profile



Version Number 1.0

June 8, 2009

SIGNATURE PAGE

Jim Robb
SWIM Governance Lead

Date

Ahmad Usmani
SWIM Program Manager

Date

Federal Aviation Administration
800 Independence Avenue, SW
Washington, D.C. 20591

DOCUMENT CHANGE HISTORY

Version	Date	Description of Changes
1.0	06/08/2009	Initial document

TABLE OF CONTENTS

1	Purpose.....	2
1.1	Scope.....	2
2	Delegation of Authority	2
3	Related Documents	2
4	Policy	2
5	Distribution	4

LIST OF TABLES

Table 1 – SIBSP Requirements.....	4
-----------------------------------	---

1 Purpose

This policy establishes the System Wide Information Management (SWIM) Interoperability Basic Security Profile (SIBSP) for all SWIM Implementing Programs (SIPs) and SWIM compliant services within the NAS. The SIBSP primarily composed from the WS-I Basic Security Profile 1 (<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>). The SWIM Interoperability Basic Security Profile (SIBSP) tailors the clarifications, refinements, interpretations and amplifications which promote interoperability found in the WS-I Basic Security Profile including the specifications. These modifications of the WS-I Basic Security Profile within the SIBSP was to improve the security and interoperability posture of SWIM implemented services and SWIM compliant services within the NAS environment.

1.1 Scope

The organizational scope of this policy covers all FAA NAS programs developing FAA SWIM compliant services within the NAS including prototypes.

The technical scope of this policy adheres to the conventions outlined in the WS-I Basic Security Profile 1.1 and mandates the adherence to this profile unless otherwise specified below.

2 Delegation of Authority

The SWIM Program Office has delegated responsibility to assess adherence and management of all SWIM Policies.

3 Related Documents

The following is a list of related publications:

1. WS-I Basic Security Profile 1.1 (<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>)

4 Policy

1. SWIM compliant services shall comply with all “MUST”, “MUST NOT”, “SHALL”, and “SHALL NOT” statements within the WS-I Basic Security Profile 1.1.

2. SWIM compliant services shall attempt compliance with all “SHOULD”, “RECOMMEND”, “RECOMMEND NOT” and “SHOULD NOT” statements within the WS-I Basic Security Profile 1.1.
3. SWIM compliant services shall comply with all of the “MUST” statements outlined below:

Requirement Number	Requirement Text	Justification
Replay of Username Token		
C4210	Any USERNAME_TOKEN that contains a NONCE and PASSWORD with a Type attribute value of "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText" MUST be referenced by a SIG_REFERENCE in order to prevent replay.	Prevents a security risk
C4211	Any USERNAME_TOKEN that contains a CREATED and a PASSWORD with a Type attribute value of "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText" MUST be referenced by a SIG_REFERENCE in order to prevent replay.	Prevents a security risk
Encryption with Signatures		
C5630	Any SIGNATURE computed over data that is subsequently encrypted MUST also be encrypted in order to prevent plaintext guessing attacks when the probable set of data values is small.	Prevents a security risk.

Table 1 – SIBSP Requirements

5 Distribution

This order is distributed to all SIPs and all SWIM compliant program offices.